ETSI

ETSI TECHNICAL REPORT

ETR 320

November 1996

Source: ETSI TC-NA

Reference: DTR/NA-006004

ICS: 33.020

Key words: IN, security

Intelligent Network (IN); Security requirements for global IN systems

ETSI

European Telecommunications Standards Institute

ETSI Secretariat

Postal address: F-06921 Sophia Antipolis CEDEX - FRANCE
Office address: 650 Route des Lucioles - Sophia Antipolis - Valbonne - FRANCE
X.400: c=fr, a=atlas, p=etsi, s=secretariat - **Internet:** secretariat@etsi.fr

Tel.: +33 4 92 94 42 00 - Fax: +33 4 93 65 47 16

Contents

Foreword

This ETSI Technical Report (ETR) has been produced by the Network Aspects (NA) Technical Committee of the European Telecommunications Standards Institute (ETSI).

ETRs are informative documents resulting from ETSI studies which are not appropriate for European Telecommunication Standard (ETS) or Interim European Telecommunication Standard (I-ETS) status. An ETR may be used to publish material which is either of an informative nature, relating to the use or the application of ETSs or I-ETSs, or which is immature and not yet suitable for formal adoption as an ETS or an I-ETS.

This ETR describes the result of security studies undertaken by ETSI Network Aspects Technical Committee (Intelligent Networks) in 1993.

Blank page

1 Scope

This ETSI Technical Report (ETR) provides the identification of the security requirements of an Intelligent Network (IN) structured network. These requirements are designed to allow a network operator or service provider to meet the following objectives:

– to operate a network or service efficiently and reliably;

– maintain customer satisfaction and good will;

– attract new business.

It is necessary to consider IN security along with reliability, service processing, management and service creation requirements to ensure comprehensive network protection.

In this ETR, IN security is considered under two categories:

1) protection of the network by ensuring that service creation, management, data and processing are properly implemented;

2) security offered in or provided by IN services.

Category 1: Security of IN protocol operations

It is concerned with the security of IN-entities: secure communication between entities and secure storage of data within those entities (or under their jurisdictions). This category concentrates on the Physical and Distributed Functional Planes. Parties involved herein are: Service Providers and Network Operators. End-Users and Subscribers are not considered at this level, but user information stored in or transported between IN entities are.

Also the interface between the management facilities and the manager and between the service creation environment and the service creator are important at this level. Inter-domain and intra-domain security aspects also belong to this category.

Mobility requirements have not fully been investigated in this ETR. When the mobility functionality is getting more mature and stable, it may require additional security requirements. This is for further study.

Category 2: Security offered in or provided by IN

This category concentrates on the Service and Global Functional Planes. The objective here is to define and specify security features and building blocks for the use in IN-services, such as an Authentication Service Independent building Block (SIB) and a User interaction SIB, which can be used for user authentication in Universal Personal Telecommunication (UPT), Universal Mobile Telecommunications System (UMTS), etc. Parties involved are: Users and Service Providers. These security SIBs and features will make use of the secured IN-entities of category 1.

The main objective of this ETR is to specify a well-balanced set of security requirements for protecting the interactions between co-operating IN entities and the path between the user and the service provider. Category 2 is for further study.

Method

A step-wise approach is used to assess and specify security, and in the early phase an attempt is made to limit the security considerations to the generic part of the IN system, i.e. category 1. A description of this method is given in annex A.

In this ETR, IN, security policy, threats and requirements are described. The next document deals with mechanisms, protocols and algorithms.

The most fundamental property of global communications is its inherent domain structure. This ETR discusses this matter in some detail. This will complement a thorough description of the IN system drawn from various sources, to identify logical components of the system and their interfaces, and the

information (messages) flowing between those components. This will provide the basis for the threat analysis in order to arrive at the security requirements.

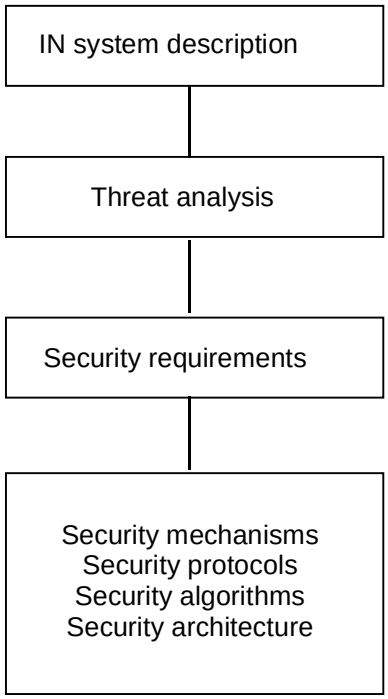


Figure 1: The various steps in specifying IN security

Organization of this ETR

The remainder of this ETR is organized according to the step-wise approach used to assess and specify security. Clause 5 describes the global IN system and identifies the various actors and the roles they may play, identify addressable system components and their functions and interfaces, and the information flowing between those components. All this information is necessary to perform a thorough threat analysis which is described in clause 6. Finally the threats are converted into security requirements in clause 7, after an assessment of the importance of the various threats that have been identified. There are three annexes to this ETR. Annex A outlines the step-wise method used to assess and specify security requirements. Annex B provides a detailed description of the IN system, and annex C provides a coarse threat analysis of the information flows between the IN functional entities.

2 References

This ETR incorporates by dated or undated reference, provisions from other publications. These references are cited at the appropriate places in the text and the publications are listed below. For dated references subsequent amendments to, or revisions of, any of these publications apply to this ETR only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies.

[1] ETS 300 374-1: "Intelligent Network (IN); Intelligent Network Capability Set 1 (CS1) Core Intelligent Network Application Protocol (INAP) Part 1: Protocol specification".

[2] ETR 318: "Intelligent Network (IN); IN Capability Set 1 (CS1) Distributed functional plane".

[3] ETR 323: "Intelligent Network (IN); Service life cycle reference model for services supported by an IN".

[4] ETR 319: "Intelligent Network (IN); IN intra domain management requirements for Capability Set 2 (CS-2)".

[5] ETR 322: "Intelligent Network (IN); Vocabulary of terms and abbreviations".

[6] ETR 232: "Network Aspects (NA); Security Techniques Advisory Group (STAG); Glossary of security terminology".

[7] ETR 083: "Universal Personal Telecommunication (UPT); General UPT security architecture".

[8] ECMA TR/46 (1988): "Security in Open Systems - A Security Framework".

[9] ECMA 138 (1989): "Security in Open Systems - Data Elements and Service Definitions".

[10] ISO 7498-2: "Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture".

[11] ISO 10181-1 to ISO 10181-7: "Information technology - Open Systems Interconnection - Security Frameworks for Open Systems".

[12] CCITT Recommendation M.3010 (1991): "Principles for a telecommunications management network".

[13] ITU-T Recommendation Q.1214: "Distributed functional plane for intelligent network CS-1".

[14] CCITT Recommendation X.509 / ISO 9594-8: "Information technology - Open Systems Interconnection - The directory: authentication framework".

3 Abbreviations and definitions

3.1 Abbreviations

For the purposes of this ETR, the following abbreviations apply:

BCSM	Basic Call State Model
B-ISDN	Broadband Integrated Services Digital Network
BRI	Basic Rate Interface
CCA	Call Control Agent
CCAF	Call Control Agent Function
CCF	Call Control Function
CCSN	Common Channel Signalling Network
CS	Capability Set
DFP	Distributed Functional Plane
FE	Functional Entity
IN	Intelligent Network
INAP	Intelligent Network Application Protocol
ISDN	Integrated Services Digital Network
ITSEC	Information Technology Security Evaluation Criteria
IWF	Interworking Function
NE	Network Element
NO	Network Operator
ONP	Open Network Provision
OSF	Operations System Function
PLMN	Public Land Mobile Network
PNO	Public Network Operator
PP	Physical Plane
PRI	Primary Rate Interface
QoS	Quality of Service
SCAF	Service Control Agent Function
SCEAF	Service Creation Environment Access Function
SCEF	Service Creation Functionality
SCF	Service Control Function
SCUA	Service Control User Agent
SCUAF	Service Control User Agent Function

SDF	Service Data Function
SIB	Service Independent building Block
SP	Service Provider
SRF	Specialized Resource Function
SS7	Signalling System No.7
SSF	Service Switching Function
STP	Signalling Transfer Point
TMN	Telecommunication Management Network
TTP	Trusted Third Party
UMTS	Universal Mobile Telecommunications System
UPT	Universal Personal Telecommunication
WSF	Workstation Function

3.2 Definitions

For the purposes of this ETR, the definitions given in ETR 322 [5] and ETR 232 [8] apply.

4 Introduction

Market pressure, deregulation of the telecommunications environment and the possible implementation of Open Network Provision (ONP), require co-operation as well as competition among the various network and service providers. This requires a high degree of standardization. It also implies that authorized operators, service providers as well as subscribers and end-users need access to management and service-providing facilities in a global distributed system.

It will, therefore, be of crucial importance and a fundamental requirement to be able to control the access to the management and service providing facilities, in order to secure the integrity and proper operation of each individual system component as well as protect their mutual interactions and to guard against misuse. This is especially so when networks and services become integrated across national boundaries and require co-operation among many individual autonomous component systems, in order to provide global services.

Laws and regulations in the various countries differ considerably. This makes it complex to develop good and efficient solutions to providing IN services, with security features, between end users.

In broad terms the main concern of security in the context of this ETR are:

- to make the users accountable for their usage of the services;
- to assure that IN functions and information are available when needed;
- to assure that the information used by any pair of IN entities is correct;
- to assure that information used by any pair of IN entities are kept confidential when needed;
- to prevent unauthorized disclosure of third party information;
- security violation should be detected and reported;
- to prevent fraud, sabotage and other misuse.

This ETR concentrates on the security aspects of the Distributed Functional Plane (DFP) and the Physical Plane (PP), or more precisely to identify threats and security requirements.

5 The IN system

This clause provides a description of the functional aspects of the IN system of importance to the assessment and specification of security. More information about the IN system can be found in annex B and in the appropriate referenced documents.

5.1 The domain structure and the need for interworking

Network interworking is a process in which several networks co-operate in providing a specific service. The need for interworking capabilities arises when a user wishes to access a service that cannot be provided by one network alone. In this context, a "network" means all functional entities and their interconnecting infrastructure that are managed by one service provider. Such a network constitutes both a management and a security domain, where the two domain borders coincide. This may not be the case in real situations. For simplicity reasons, fully coinciding management and security domains are assumed in the following.

It is assumed that each domain is, to a large extent, autonomous with respect to defining its own security policy, the security facilities needed to implement the policy, and the security mechanisms required to realize those services.

The situation is illustrated in figure 2. The figure identifies three main interaction paths between the domains. They represent different types of interactions between different pairs of entities in the domains involved. Hence these interactions may contain signalling information or various kinds of management information, all transferred over the same common communications infrastructure called the Common Channel Signalling Network (CCSN).

Since each domain is autonomous and responsible for its own management security, each domain will apply the means necessary to protect its own resources and its own integrity. Laws and regulations in the different countries may require different means of protection for different kinds of information. An example here is information relating to individuals, like identity, location of calls, call destinations and charging information. In one country such information may require complete confidentiality by means of the application of for example a national cryptographic algorithm, while in another country such protection may be optional or even prohibited.

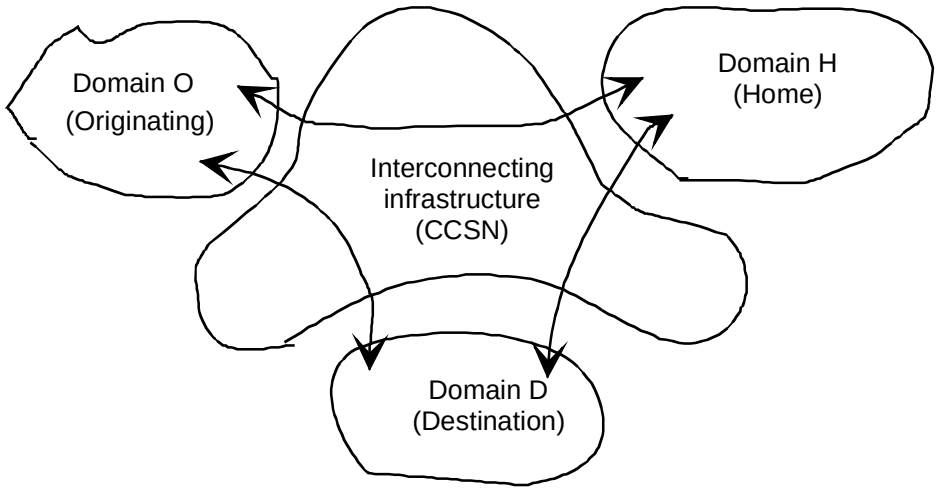


Figure 2: Interaction paths between IN domains

The protection measures, i.e. the security mechanisms and services to apply in a domain is prescribed by the security policy for that domain. This incorporates also all interfaces that can exchange information with other domains, to provide services to these domains or to make use of services provided by the other domains. In the following, such an interface is called an external interface, to distinguish it from an interface for internal use (intra-domain).

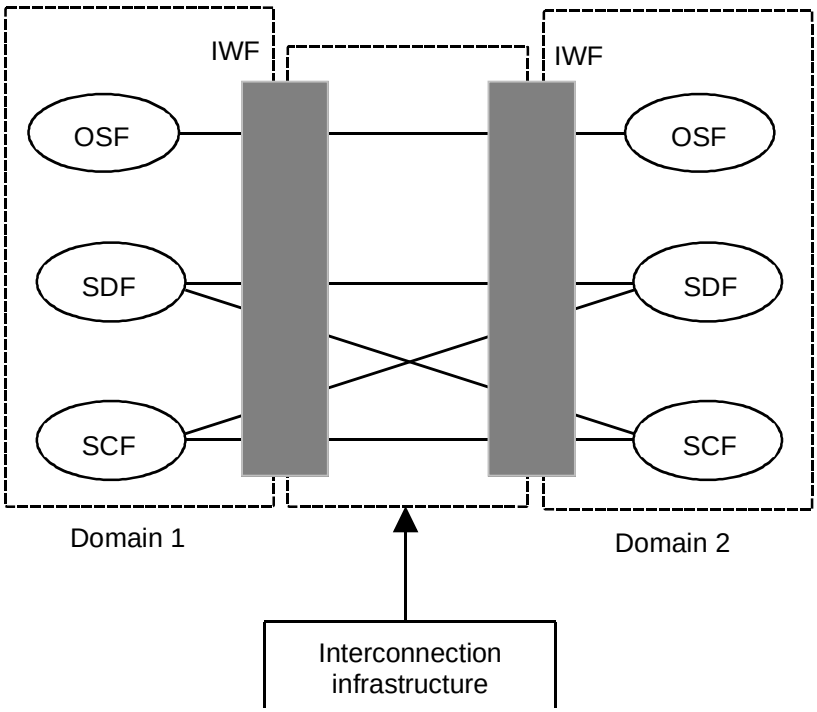


Figure 3: Interworking relationships for service executions and service management in Capability Set 2 (CS2)

Currently the following service execution relationships are considered for interworking in CS2, see figure 3:

- Service Control Function - Service Data Function (SCF-SDF);
- SCF-SCF;
- SDF-SDF.

The figure also includes the Operations System Function - Operations System Function (OSF-OSF) relationship. Protection of this relationship has been studied in CCITT Recommendation X.509 [14] and is taken care of in the Telecommunication Management Network (TMN) architecture, hence it is outside the scope of this ETR and not considered in the threat analysis.

The Interworking Function (IWF) can be modelled in two ways, either as an integral part of each of the above-mentioned entities, or as a separate entity that can be used by all entities in need of interworking functionality. In the latter case, the IWF needs to contain switching (routing) capabilities to direct the information flow to and from the correct IN entities. This is the model adopted in this ETR.

The IWF should be service independent.

5.2 Actors and roles

There will be several actors involved in providing and using IN services. In the following, a short description of the roles these actors may have in the provision of IN services is provided:

- Network Operators (NOs); both public and private network operators are considered. Normally they will be located in different management (and security) domains. In a given call situation, a NO can act either as an Originating, Terminating, or Transfer NO. A NO may provide network services to other NOs, to Service Providers (SPs) or to end users;
- SP; each SP will normally constitute a domain on its own with respect to management and security. In a given call situation, four different domains can be distinguished: the originating domain, the home domain, the terminating domain and possibly one or more intermediate domains. A SP makes use of network services provided by a NO and can provide services to other SPs and to subscribers and end users;

- subscribers; the legal body subscribing to and paying for an IN service, but not necessarily making directly use of that service;

- end User; the ultimate user of IN services. In many cases the end user will also be the subscriber;

- Trusted Third Party (TTP); an actor that provides trusted services to other parties, like name to address conversions (standard directory services), key (generation) and distribution, authentication service, certificate distribution and non-repudiation services (notaries functions, etc.).

The service creator will be an actor that needs to be considered in a future study.

5.3 IN management

IN management functionality will be used to provide and manage service creation, the service control functionality, service data functionality, specialized resource functionality and the combined service switching/call control functionality in the network, outside the context of call/service processing. The IN management functions are modelled according to the TMN functional architecture. The end user may access management facilities via a Workstation Function (WSF) and a direct link to the TMN system, or as part of management features implemented in the SCF service logic. The entity OSF in figure 4 should be seen to represent the full TMN capability, including Element Management, Network Management and Service Management functionality (E-OSF, N-OSF and S-OSF, respectively).

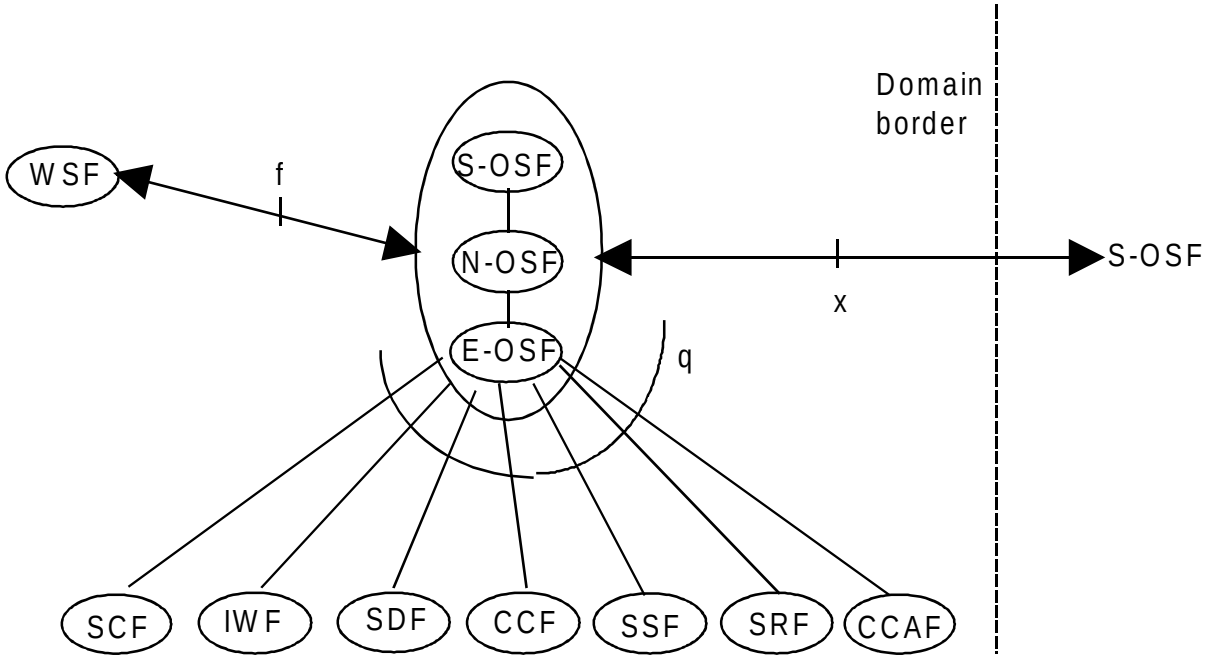


Figure 4: Relationships between the management functionality and the IN entities

The thin solid lines in figure 4 illustrates the relationships between the management functionality and the various IN entities. The Operations System Function - Call Control Agent Function (OSF-CCAF) and Operations System Function - Call Control Function (OSF-CCF) interactions shown in figure 4 reflect the integration of management of IN services and management of the basic call functionality.

There are two aspects of IN management. The first one is based on TMN functionality. The other one is part of the repertoire of IN service features. In the context of this document, IN management means capabilities based on TMN. Such functionality is currently not accessible to the IN end user, only via workstation functionality directly connected to the TMN system. Management manipulations performed via IN service features will be part of the normal IN operations and considered in that context.

The user access to Service Creation Functionality (SCEF) will be controlled by a Service Creation Environment Access Function (SCEAF), which most likely will be managed by the OSF. In this context, the user is the person developing/creating the various components of the IN service. It seems very unlikely that the IN end user will be permitted to access the SCEF. The IN Service Management

Functionality is in the figure represented by a combination of Element Management, Network Management and Service Management functionality (E-OSF, N-OSF and S-OSF, respectively). It is not clear if the user should be able to access the Service Creation Environment via service management functionality (S-OSF). The security aspects of service creation is for further study, and will most likely add on its own specific security requirements.

5.4 The modes of communications between IN entities

Two typical modes of interactions can be identified at first glance:

- transactions or request-response like interactions, providing updates of management information, logging information, or command-response. Such interactions may be based on connection-oriented or connection-less mechanisms in the signalling network (CCSN);

- file transfer, providing transfer of larger amount of information like user profile information, user-specific accounting information, etc. Such interactions will most likely be based on a connection-oriented transport service.

The mode of communication will have no or little effect on the security requirements, but most likely have effect on the choice of security solutions to fulfil these requirements.

6 Threat analysis

6.1 Introduction

ETR 323 [3] consists of the following phases: Service Creation, Service Enabling, Service Subscription and Service Invocation/Activation. Before a particular service can be invoked, it needs to have been created, made available for invocation and been subscribed to by the user. After a particular service has been invoked and used, it is terminated and the user will later be charged for its use. The user may later decide to withdraw his subscription to that service, or the SP may choose to disable the service and not make it available for subscription and use. The service creator may also choose to remove the service totally.

Each of these phases are susceptible to various threats and should be analysed carefully in order to specify the necessary security requirements and the countermeasures. This is a considerable task. Service creation and enabling may partly be considered as separate activities and partly as integrated with management. This ETR concentrates on the invocation phase. Later, when the creation and enabling processes are more mature, these phases need a careful evaluation.

In analysing the threats to an IN system, the problem is divided into three distinct areas:

- the standard IN control relationships inside one provider's domain;

- the management relationships;

- the interworking relationships.

Figure 5 illustrates the service control relationships as defined in CS2 so far. The OSF entity stands for the whole management functionality relevant to the management of an IN system.

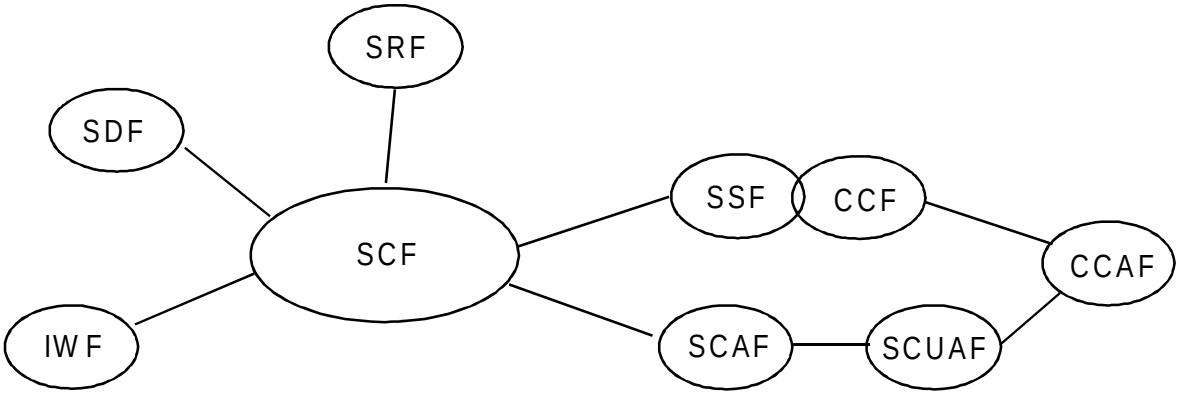


Figure 5: Standard IN relationships inside one domain to consider in the threat analysis

Figure 6 depicts the relevant management relationships. The service creation environment is not considered here, but as mentioned previously it will be studied later when that process is better understood.

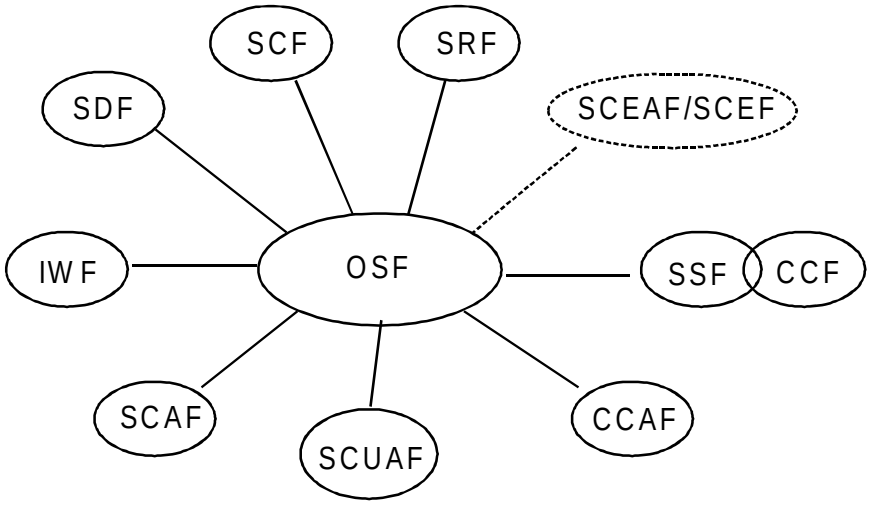


Figure 6: IN management interactions to consider in the threats analysis

The management relationships with OSFs in other domains are also excluded, since the analysis of threats to those and the specification of countermeasures are part of the X interface and already handled in CCITT Recommendation M.3010 [12].

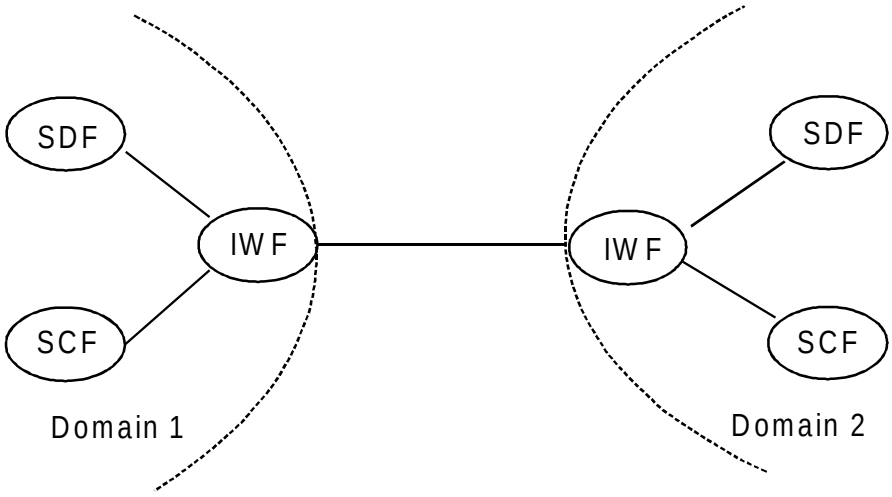


Figure 7: The interworking relationship to consider in the threat analysis

Since dedicated interworking entities have been chosen, there is only one interworking relationship to consider in the threat analysis, as shown in figure 7.

6.2 Threat analysis of IN relationships inside one domain

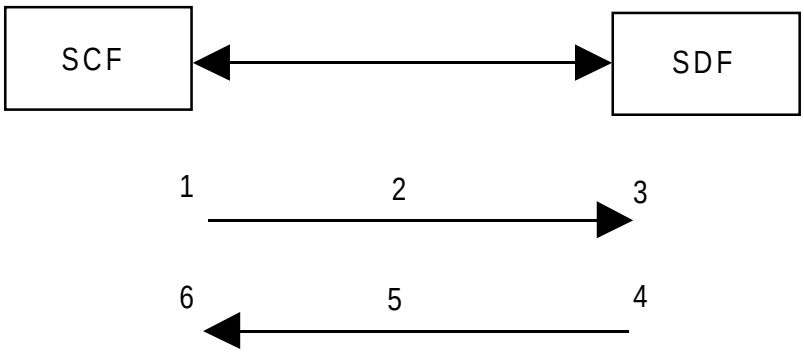
The first section outlines the generic threats and risk picture for any IN relationship, using the SCF-SDF relationship as an example. It is believed that the identified threats to this relationship in general will be representative for all other relationships. Then follows some considerations regarding the Specialized Resource Function - Service Control Function (SRF-SCF) relationship. This is rounded off with a concluding section, based on an analysis of the Core Intelligent Network Application Protocol (INAP) messages. The details of this analysis can be found in annex C.

6.2.1 Generic threats to IN relationships

In the following the SCF-SDF relationship is used as an example of a threat analysis. Both entities are located within the same domain. It is further assumed that this relationship can be infiltrated by an intruder. For the purpose of this analysis it is also assumed that there is little mutual trust between these entities. In reality the vulnerability to these threats will greatly depend on how these entities are being realized/implemented.

Functionality

With respect to the SCF-SDF relationship the following steps in the interaction are identified (see figure 8).



1) SCF creates a request for information (to send to SDF).
2) The request is sent to SDF.
3) SDF receives the request and processes it.
4) SDF formats a response with information (to send to SCF).
5) The response is sent from SDF to SCF.
6) SCF receives the response with the requested information and processes it.

Figure 8: SCF-SDF interaction steps

The information requested and sent will often be user related information like:

identification, registration information, security parameters, etc.

Threats

The following threats are identified for the steps 1 through 6:

1) SCF creates a request for information (to be sent to SDF):

   a) the request made can, intentionally or unintentionally, be extended beyond the authorization level; SCF attempts to extract more information from SDF than it is authorized for.

2) The request for information is sent from SCF to SDF:

   a) the request can be modified during transmission;

   b) the contents of the request can be eavesdropped during transmission;

   c) the request can be blocked (e.g. to enforce a lower level authentication procedure, which is applied to avoid denial of service to the user).

   NOTE 1: In this case the security of the IN model could influence the security of an individual service.

3) SDF receives the request and starts to process it:

   a) the contents of the request may not be authentic; e.g. the request has been modified during the transmission;

   b) the sender of the request may not be authentic; e.g. a false request has been inserted by an intruder;

   c) replay of a previous legal request by an intruder.

4) SDF creates a response with information (for sending to SCF):

   a) the response created may be non-genuine (e.g. SDF provides false information).

5) The response with information is sent from SDF to SCF:

   a) the response can be modified during transmission;

   b) the contents of the response can be eavesdropped during transmission;

   c) the response can be blocked (e.g. to enforce lower level authentication procedure, which is applied to avoid denial of service to the user).

   NOTE 2: In this case the security of the IN model may influence the security of an individual service.

6) SCF receives the response with information and starts to process it:

   a) the contents of the response may not be authentic; e.g. message modification;

   b) the sender of the response may not be authentic; e.g. message insertion.

Risk analysis

The risk evaluations follows the functional steps previously identified:

1a) impact difficult to estimate; apply outgoing access control that will be controlled by the current security policy;

2a) no practical direct gain seen;

2b) medium threat with respect to privacy, could be high for certain services (if e.g. information is reusable);

2c) could be serious threat - impact depends on service; related to service availability;

3a) low risk, assuming the SDF provides no secret information in the resulting response which may be eavesdropped;

3b) high risk if this leads to providing information (even though not secret) to an incorrect entity;

3c) low risk, assuming the SDF provides no secret information in the resulting response which may be eavesdropped;

4a) seems not to be very realistic; counter measures on legal/security policy level. May result in an accountability problem and corrupt the billing process;

5a) high in case of authorization information. Other reason: denial of service;

5b) low risk, assuming the response contains no secret/private information;

5c) could be a serious threat - impact depends on service; related to service availability;

6a) high in case of authorization information;

6b) high in case of authorization information. May result in an accountability problem and corrupt the billing process.

6.2.2 Threat analysis of the SCF-SRF relationship

The SRF is seen as an interface between the end user and SCF. The same assumptions about the SRF-SCF relationship are made as for the SCF-SDF. The threats to this relationship will, therefore, be very similar to the one for the SCF-SDF relationship.

All call/user related information stored in or transferred to and from the SRF shall be protected.

The user-SRF interface is not considered in this ETR. This interface may have security aspects that need to be studied.

6.2.3 Sensitivity of the Core INAP Information Flows

Table 1: Content sensitivity in Core INAP

w15 from → to	SCF	SSF	SRF	SDF
SCF	not yet defined	Medium	High	High
SSF	Medium	N/A	N/A	N/A
SRF	High	N/A	N/A	N/A
SDF	High	N/A	N/A	not yet defined

Most of the Core INAP messages are vulnerable to masquerade, modifications and disclosure, as can be seen from the summary in table 1. More details on these matters can be found in annex C. The analysis is only covering CS1 and needs to be extended with the additions for CS2.

The risk of being compromised is very difficult to evaluate. In most cases the INAP messages carry user/subscriber related information, or may enable unauthorized traffic analysis. Therefore, these messages need to be protected, to protect the privacy of the users/subscribers and to protect the provider against the disclosure of business competitive information.

6.3 Threats to IN management

Potential threats to the various management relationships will be very similar to those described above. The vulnerability to these threats will depend on the practical realization of the IN system including the management capabilities. The consequences of being compromised have to be worked out. This will be for further study.

There are two areas of threats to IN management that need to be considered:

- threats to the access to management capabilities;

- threats to the various management relationships.

The latter area have a very similar threats picture as the one described for the standard IN relationships. The threats in the first area are coupled to the identification of the users, the roles they may play in relation to the management capabilities and to control their privileges. This will be for further study.

6.4 Interworking threats

Potential threats to the various interworking relationships will be very similar to those described above. There is certainly less trust between interacting IN components located in different domains compared to when all entities are in the same domain. The risk analysis provided in subclause 6.2.2 is also valid for the interworking relationships, but the degree of hazards is likely to be higher. The consequences of being compromised have to be worked out. This will be for further study.

6.5 Conclusions

As illustrated in figure B.1, global IN systems are highly distributed systems involving many individual domains that are practically autonomous with respect to management and security. Based on the threat analysis, a first conclusion can be stated:

– interworking relationships are in general exposed to a greater variety of treats than relationships internal to a domain;

– the likelihood that a particular threat to an interworking relationship will be realized, i.e. that a certain weakness will be detected and exploited by an unfriendly party, is higher than for the same relationship internal in a domain.

The potential threats to any pair of interacting IN entities are summarized below, see figure 9. In a particular relationship, one entity is taking the initiative to request one or more services (actions) from the other one. With respect to the potential threats it makes not much of a difference whether the entities are located in the same provider domain or in different ones. But the likelihood that a particular weakness will be exploited, will depend upon the location of the intruder, the effort of exploiting the weakness and the potential benefit the intruder can gain from his action.

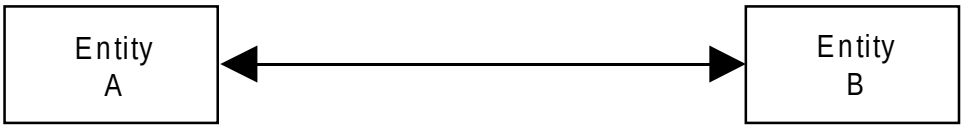


Figure 9: Two co-operating IN entities

The most obvious threats are:

a) One entity masquerades as another legitimate one and thereby gains access to the services provided by the other one (and vice versa) and thereby initiate actions or get access to information it is not authorized for.

EXAMPLE 1: Masquerade as a SCF to retrieve information from a SDF.

EXAMPLE 2: Masquerade as a SRF to retrieve information from a User (ID, authentication code, etc.).

EXAMPLE 3: Masquerade as a SCF to control a Service Switching Function (SSF) of another provider.

b) The fabrication, modification, replay, reflection or deletion of messages (protocol data units) flowing between IN entities.

EXAMPLE 4: Modification of location, charging or authentication data in messages.

EXAMPLE 5: Modification of an authentication response message from a SDF.

EXAMPLE 6: Modification of a message to lower the security level or to obtain. more information from a SDF.

EXAMPLE 7: Replay of previously exchanged messages, with the intention to impersonate as another entity or user.

c) Disclosure of parts of or whole messages exchanged between IN entities.

EXAMPLE 8: Eavesdropping of personal data, business competitive data or authentication data carried in messages exchanged between a SCF and a SDF, or between CCF-SRF-SCF.

d) Unauthorized access to IN facilities (functions and information) within the jurisdiction of one IN entity (Server).

EXAMPLE 9: Entities acting outside their privileges; a legitimate SCF modifies its privileges at a SDF from *read* to *read/write.*

EXAMPLE 10: A legitimate SCF extracts more information from a SDF than it is authorized for.

e) Denial of service.

EXAMPLE 11: Blocking of authentication checks to enforce a lower security level.

EXAMPLE 12: Blocking of message access to a given entity.

f) Repudiation:
(Denial by one party that it was the originator of a particular message);
(Denial by one party that it was the recipient of a particular message).

EXAMPLE 13: Denial by an entity that it has initiated an action or made use of a service.

EXAMPLE 14: Denial by a service provider that it has refused to provide service to a legitimate service user (provider or end user).

7 Security requirements

7.1 Introduction

This subclause starts with specifying the baseline security requirements for global IN systems. These requirements should be fulfilled by any capability offered by an Intelligent Network. Then more detailed specifications of the requirements are described, which follow the same subdivision as in clause 6, by grouping the requirements according to their intra-domain aspects, service management aspects and interworking aspects. Some of these requirements depend upon the evolving IN architecture, and can, therefore, not be specified currently. They are, therefore, for further study.

7.2 Baseline security requirements

The process of making a system secure proceeds along different directions:

- to limit the functionality of the system to what is absolutely necessary and to limit the possibility to access the system;

- to reduce the potential threats to the system by strictly controlling the access to the functionality and to stored and transferred information;

- to provide functionality that detects security violations or attempts to break the security and that enables corrective actions after security has been violated;

- to ensure that lawful interception of user communications be possible in accordance with national laws.

The first bullet item is mainly a system design issue, while the other three are tightly coupled to the application of security services and mechanisms. The most basic security requirements will be the following.

Accountability:

Accountability means that a user or any entity acting, directly or indirectly, on behalf of the user, should be responsible for any actions initiated by, or on behalf of, the user.

There are three aspects of accountability to consider in the IN context:

a) user/subscriber accountability;
b) IN provider to IN provider accountability; and
c) an IN provider to network operator accountability.

Item c) is for further study.

Accountability can be achieved by applying authentication, access control and integrity. This implies that prior to using a particular service, the service using party should be registered as a legitimate user/subscriber at the service providing party. Depending on the degree of mutual trust between the user/subscriber and the service provider or between service providers, more or less complex facilities are needed to resolve repudiation conflicts.

Availability:

As for accountability, there are three aspects of availability to consider in the IN context: a) user/subscriber to IN provider availability, b) IN provider to IN provider availability (interworking aspects), and c) IN provider to network operator availability. All legitimate users or entities that make use of IN or network services, functions or information, should experience similar and fair access to those facilities. For the most parts, availability will be an issue related to reliability aspects in network and service design and, therefore, is outside the scope of this ETR. This ETR focuses on a) and b), while c) is for further study.

Integrity:

When a legitimate user/subscriber invokes a particular service, that service requires a certain Quality of Service (QoS) as part of the subscription contract between the subscriber and the service provider. Any attack on the service or network resources reducing the QoS can implicitly be viewed as a compromise of the integrity and availability of the system, and therefore needs to be counteracted.

It is, therefore, of concern to an IN provider to ensure that his system operates correctly both internally and in co-operation with other IN service providers and with network operators. This means that any interaction between any pair of IN entities internal to the IN provider or located at different providers, or between IN entities and network operator entities, should be adequately protected.

In addition an IN provider will require that co-operating IN providers and network operators can assure that their systems will operate properly. This shall be specified as part of the co-operation contract between the involved parties.

Confidentiality:

It may be required in certain situations to keep information confidential and in other situations it may by optional. Confidentiality is needed to protect personal related information, business competitive information and the like. In general all third party related information will require protection both from disclosure and manipulation. Information could be disclosed because:

- no confidentiality facilities are provided for transported data;

- the structure of the system and the pattern of total information flows may permit inference of certain information, for example traffic analysis with business competitive aspects;

- access control could be circumvented (e.g. database access via operating system routines instead of via INAP);

- a masquerading entity is given information to which it is not entitled;

– one or more system entities are tampered with to behave in a modified way (for example illegal interception and copying of messages);

– of direct observation of an unprotected interface.

Security violation detection:

There should be capabilities for logging and processing security relevant activities, and generate alarms when certain conditions or thresholds are reached. The IN provider shall be alerted when security is violated intentionally or unintentionally, for example when unlawful interception has been detected. A User/Subscriber may be alerted. The conditions for alerting a User/Subscriber will depend on the policy of the IN provider and the type of violation. When security is violated or a breach in the security has been detected, there should be capabilities to restore the system to its secure state.

Lawful interception:

Interception of user communications or any attempts to do so, whether lawful or otherwise by organizations who have legitimate reasons for interceptions, by means of devices and/or via interfaces both of which are:

- placed by the network operators or service providers at the disposal of the national law enforcement agencies according to national laws; and

- intended solely for lawful interception purposes,

shall be monitored and registered in accordance with the national laws.

7.3 Security and the mode of interaction between IN entities

As mentioned previously, the connection or association between interacting IN entities can either be connection-oriented or connection-less. The connection mode will have some implication on security. In the connection-oriented mode it is usual to apply mutual authentication. This means that both interacting entities require to verify the identity of its counterpart at connection establishment time. The mutual authentication, or peer entity authentication, is only valid for the point in time where it is performed, and should be augmented with additional security facilities like integrity and/or confidentiality to be valid for the whole duration of the connection. For connection-less interactions, the authentication will only be one-way, i.e. origin authentication. That means that the side receiving a message (packet) will be able to verify the identity of the originator of that message. Hence the authentication is only valid for that message. Consecutive messages therefore should be individually authenticated.

7.4 Security requirements for co-operating IN entities inside one domain

This subclause presents security requirements for IN relationships. These requirements are based on the results of the preceding clauses. These results can be summarized in the following security objectives:

The IN needs to be protected against:

- unauthorized use of services and resources;

- unauthorized disclosure of stored or transferred data;

- unauthorized modification, replay and deletion of data;

- denial of service.

These objectives can be met by applying security facilities in the IN architecture. Security facilities are implemented by security mechanisms. In some cases different security facilities can be implemented by one single security mechanism (e.g. a Message Authentication Code (MAC) mechanism can provide both "Data Origin Authentication" and "Data Integrity").

Authentication is required between all Functional Entities (FEs) in order to protect the entities against masquerade by other entities or intruders. The feature "Data Origin Authentication" can be used between most of the FE. Else peer-to-peer authentication shall be required.

Audit and alarming is required for each communication activity between FE. Misuse shall be detected and reported. Audit helps to check the system against unwanted and unaware activities or possibilities in the system.

Data integrity is required to give protection against unwanted modifications, deletion and additions. Messages sent between most FE are vulnerable to these threats, according the threat analysis, and shall therefore be protected.

Access Control is required to protect against prohibited access, and disallowed and unwanted activities in the FEs.

Confidentiality is required to protect against disclosure of information, either stored or in transfer. Probably confidentiality is not necessary for all information and could therefore be selective: at least all user-related data (user profiles) coming from and sent to SDF and SRF should be protected.

Non-repudiation is mainly required on relationships and interfaces crossing domain borders and between SCF and SRF, to protect against denial of having sent or received information. Depending on how the IN functional entities are being realized inside a particular domain, other relationships may also be considered for non-repudiation services.

Table 2 shows a summary of these requirements for each IN-relation.

Table 2: Security requirements and FE interfaces

	data orig authent.	**peer-ent. authent.**	**audit & alarm.**	**data integrity**	**access control**	**selective confid.**	**non-repud.**
rw15 SCF-SCF	x	-	x	x	x	x	-
SCF-SDF	x	-	x	x	x	x	-
SDF-SDF 2)	x	-	x	x	x	x	-
SCF-SRF	x (note 1)	-	x	-	-	x	-
SCF-SSF	x (note 1)	-	x	-	-	-	-
SCF-OSF 2)	x	-	x	x	x	x	x
OSF-SDF 2)	x	-	x	x	x	x	-
OSF-SRF 2)	x	-	x	-	-	x	-
OSF-SCEF 2)	x	-	x	x	x	x	x

NOTE 1: Particularly important in the case of inter-domain relations.

NOTE 2: From a security point of view this relation is not recommended for inter-domain communication.

7.5 Security requirements for IN management

Security requirements are divided in two groups.

Access to management functionality:

- authentication of the user;
- perform access control based on the verified user identity and his/her management role;
- management requests may need integrity checks;
- some management requests-responses may require confidentiality.

Some of the security facilities used to implement these requirements may be combined with those used to authenticate users in connection with the invocation of normal IN services.

Requirements for the various management relationships:

- ensure the integrity of each relationship; meaning that the communication entities are the correct ones and that the exchanged information is correct (integrity checked). This requirement may imply authentication of the communicating partners, and will to a great extent depend upon the environment in which the entities operate;

- access control;

- some management exchanges may require confidentiality.

These requirements are for further study.

7.6 Security requirements for the interworking function

The security requirements for the IWF consists of the requirements as described in subclause 8.4 and of additional requirements due to the inter-domain interactions. Consider for example the SCF-SDF relationship. Two situations are identified:

1) their mutual interactions are end-to-end and terminate in the SCF and the SDF entities, respectively. The IWF will then be transparent to the SCF-SDF communications, and acts as a Signalling Transfer Point (STP) and just relay the information;

2) their mutual interactions proceed basically in three steps; SCF-IWF, IWF-IWF and IWF-SDF. Each step corresponds to a set of exchanges terminated at application level. This option will be used where it is necessary to convert between different signalling and protocol systems.

The security requirements for Option 1 are:

- authentication of the communicating IWF entities;

- all relayed information shall be integrity protected;

- all relayed information shall be confidentiality protected as default. Optionally this feature could be turned off between selected pairs of IWFs;

- access control is performed by filtering on the originating and destination addresses. Hence the IWFs can not perform any end-system application-related access control. If this feature is found necessary, it has to be built into the co-operating systems themselves.

The security requirements for Option 2 are:

- authentication of the communicating IWF entities;

- all information exchanged shall be integrity protected;

- all information exchanged shall be confidentiality protected as default. Optionally this feature could be turned off between selected pairs of IWFs when desired;

- access control performed at application level by means of access control lists or capabilities.

7.7 Fraud management

Fraud management consists of several elements, for example analysis of historical data (audit information) to detect abnormal patterns, misbehaviour and abuses, and with this knowledge to try in real time to detect and filter out new attempts to abuse the system. Fraud management is user and service related, and can be considered to be on the border between Category 1 and Category 2.

Fraud management will be for further study, but some initial requirements are given here.

Fraud detection

Any systematic attempt to get unauthorized access to user accounts, or in an unauthorized way to block one or more user accounts, shall be detected, the account holders notified when this is in line with the security policy of the provider, and the appropriate steps taken to correct the system.

A usual procedure to protect a specific user account is, when the number of failed attempts to authenticate an account number exceeds a given threshold, to block the account and notify the account holder.

A few example on how the security of such accounts can be violated, are given below:

- for a given account, systematically cycle through the authentication code space until blocked;

- for selected authentication codes, cycle through the account number space to find matching account numbers;

- malevolently block one or a set of accounts by systematically authenticate falsely until the accounts are blocked.

Credit limits

When a subscriber opens an account, and especially if it is a Charge Card account, there shall be an option to set a credit limit on the account. The credit limit may be on a day-by-day basis, on a weekly basis, or provide an overall limit. This will limit the damage, if abuses take place.

Origin and Destination limits

Another security measure will be for certain Charge Card accounts (for new or less trustworthy subscribers) to limit the destinations of calls. The limit may be within a given area, within the country, or even only to a specified destination address. Likewise, a limit may be put on the callers location when calls are made.

Annex A: The process of assessing and specifying security in IN

Figure A.1 illustrates all the steps in the process of specifying security for a given system.

A.1 Strategic security requirements

As a starting point for the development of secure IN systems, the following strategic security requirements can be stated:

- the information exchanged between any pair of IN entities shall be correct;
- IN functions and information shall be available when needed;
- the user of a given IN service shall be accountable for it;
- information exchanged between IN entities shall be kept confidential when needed;
- security violations shall be detected and reported;
- ensure that lawful interception of user communications is possible and in accordance with to national laws.

These strategic requirements will be a guide for the identification of all important threats as an intermediate step in specifying security.

A.2 Regulations

European laws and regulations will have several effects on the security requirements. In most countries it is required to protect the privacy of users. That means that information related to users stored within the IN network or being transferred across the network, need to be kept confidential. The use of cryptographic methods may not be restricted in some countries, while in others are prohibited or severely restricted. Provisional guidelines can be found in the European Union document "Amended proposal for a council directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (SYN 287, 1992)". For IN, special concerns in this respect should be paid to the contents of personal data stored in the SDF and transported from and to the SDF. If the evolving concepts of ONP is being implemented, it will require that certain interfaces are openly accessible, and hence increase the need for security.

A.3 System description

Describe the architecture and functions of the system, focusing on the following properties:

- functional description of each system component and its interface(s). It will be useful to distinguish between generic and service specific functionality and between intra-domain and inter-domain functionality;
- what kind of information is stored where in the system, either permanently or temporarily, and its importance to the correct functioning (integrity) of the system and to the privacy requirements of the system's subscribers and users;
- the sequence and meaning of the information flows between the system components;
- identify the borders of responsibilities with respect to system management and service provision;
- describe the customers of the services offered by the system, i.e. other service providers, subscribers and end-users, and their access rights to functions and information in the system (the access policy);
- identify and describe the level of trust between co-operating IN provider systems and how disputes about service offerings and service usage should be resolved, i.e. the need for trusted third party to provide a non-repudiation service.

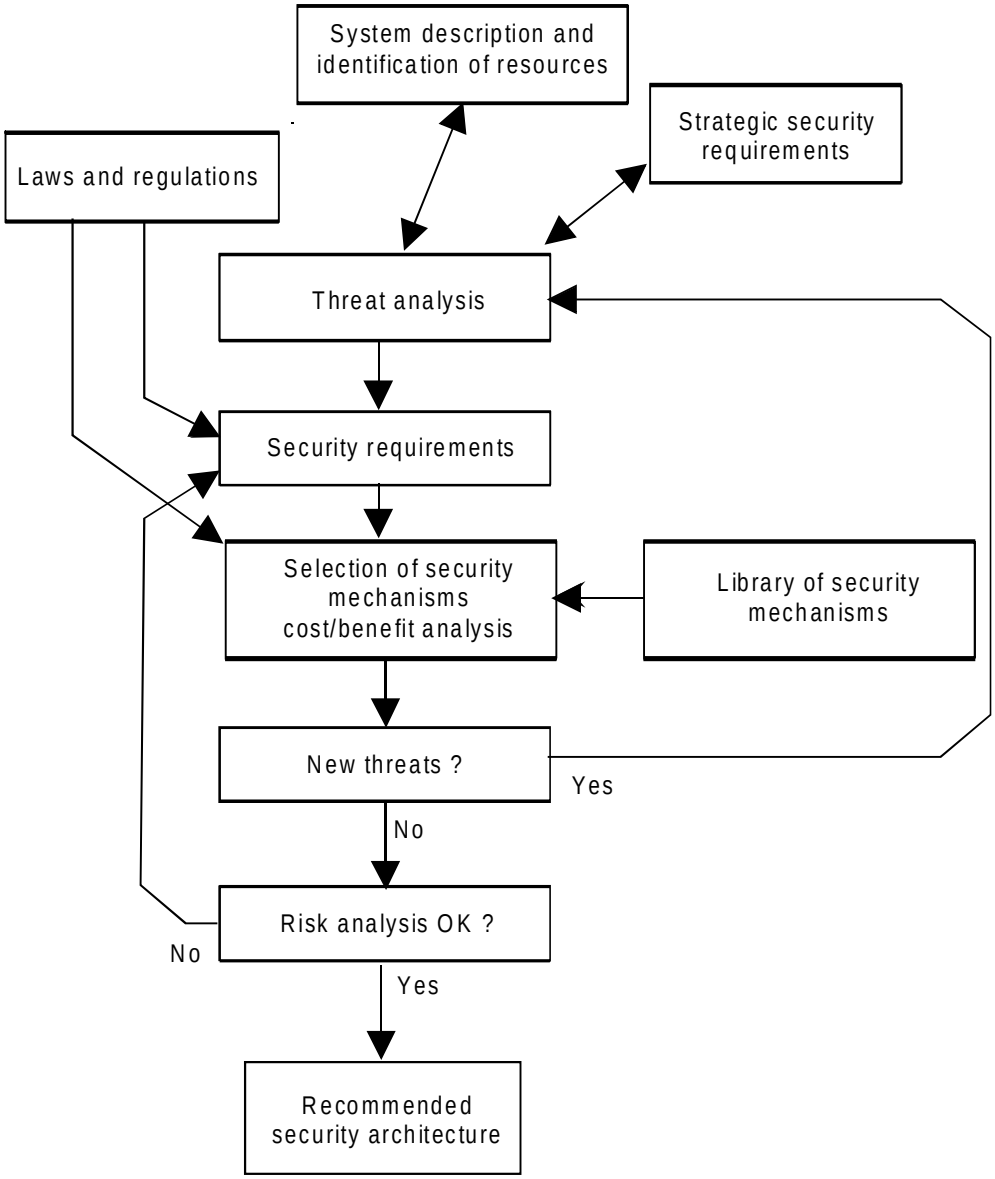


Figure A.1: The steps in assessing and specifying security

- how should an end-user registered in a remote system (domain) be made accountable for its utilization of a particular service. Should this be done directly, meaning that the system should know the identity of the user and be able to verify its correctness. Or can this be delegated to the remote system?

- describe the security management requirements for the system;

- provide some insight in how the system will be realized physically;

- for what purpose(s) will the system be utilized, i.e. what is the value of the information that will be transported around by the system, like funds transfer, booking information, industrial information and private communications;

- any evolutionary aspects of the system that may affect the choice of security solutions.

A.4 Threat analysis

A potential threat to (or a weakness in) a system is doing no harm until the point in time when the weakness is exploited by an intruder. The likelihood that a particular weakness will be exploited, will depend on many factors like: the physical realization of the system, the location of the intruder, the expenses and effort the intruder has to invest to exploit the weakness and the potential benefit the intruder

can gain by his action (or in the negative sense the amount of damage done to the system). The latter will strongly depend upon the applications the system is used for.

Hence a careful analysis of all the threats that can be identified should be performed, ranging the threats in order of importance. This may be difficult, since the various aspects of costs can only be roughly estimated. In evaluating each potential threat, an attempt should be made to characterize it according to:

- the likelihood that a weakness will be detected. This will to some extent depend upon the location of the intruder relative to the weakness;

- the cost and effort involved in exploiting the weakness;

- the potential benefit gained by the intruder in exploiting the weakness;

- the potential damage that can be done to the system and its actors (and its subscribers/users).

A.5 Security requirements

Based on the ordered list of threats, the security requirements can be specified, i.e. to convert threats into requirements. In addition, security requirements imposed by the Commission of the EU and by national legislation's and regulations in the various European countries need to be taken into account.

A.6 Selection of security mechanisms and cost/benefit analysis

In order to perform this step in the assessment and specification process a library of security mechanisms is assumed, ordered according to the security services they can be involved in:

for each security service,
do describe all applicable security mechanisms and their figures of merit like:
- effect on system performance;
- effect on user friendliness;
- cost of implementation;
- cost of management.

For each security requirement, perform a cost/benefit analysis to select the most cost effective security mechanism to counteract the threat. Cost means not only the real costs, but in a broader sense, also the side-effects on performance, user friendliness, etc. The choice of security mechanisms will also be affected by national legislation and regulations. The potential damage and economical loss the provider may experience when the weakness in the system is being exploited is not incorporated at this stage. But this should be taken into account by the relevant parties themselves.

As a side-effect new threats may be created in the process of selecting the proper security mechanisms:

if new and significant threats were introduced in the selection process,
go back to **Threats Analysis** and update the list of threats,
then proceed from **Security Requirements**,

A.7 Risk analysis

Normally at this stage, there are some residual threats left, which have not been accounted for.

Based on the known residual threats, a risk assessment needs to be performed to provide an estimate of the potential economical damage to the service provider and the loss of reputation if the integrity of his system and services are being compromised:

if the risk is not acceptable,
go back to **Security Requirements** and update the security requirements;
then proceed from **Selection of Security Mechanisms**.

A.8 The security architecture and security management

The result of this step-wise approach will be a set of security mechanisms. These have to be integrated into a coherent security architecture as part of the IN architecture. It may also be necessary to provide a guideline to this architecture, in line with what has been done in Information Technology Security Evaluation Criteria (ITSEC). Having the security architecture in place, the means to manage the various security elements of the system can then be developed. It needs to be kept in mind that a European-wide system comprises many individually managed provider systems that to a large extent are autonomous with respect to security.

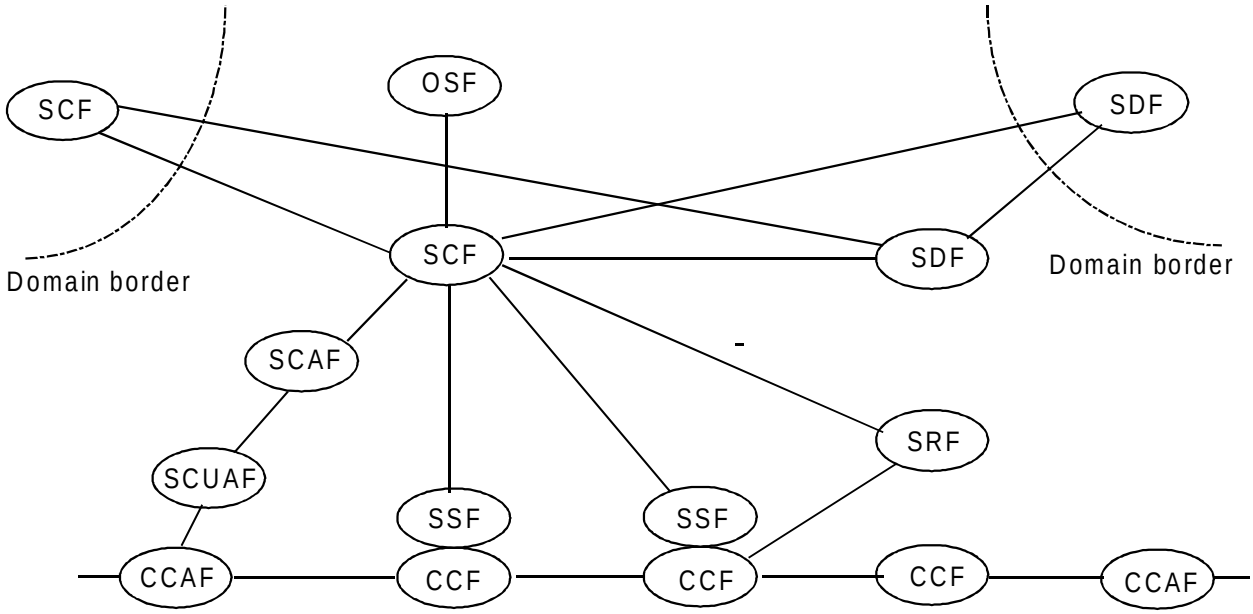
Annex B: Detailed description of the IN system

This annex provides a functional description of the IN system and each of its component, taken from ITU-T Recommendation Q.1214 [13] and ETR 319 [4].

B.1 General functional description

It is worth mentioning that the architecture is not yet in its final form, and therefore may change with time. Figure B.1 depicts the main components of the CS2 architecture and their relationships. The scope of the functionality is to provide:

- end user access to call/service processing;
- service invocation and control;
- end user interaction with service control;
- IN management;
- inter-working between service processing functional entities.



CCAF: Call Control Agent Function
SCAF: Service Control Agent Function
SCUAF: Service Control User Agent Function
CCF: Call Control Function
SCF: Service Control Function
SDF: Service Data Function
SRF: Service Switching Function
OSF: Operations System Function

NOTE 1: IWF has been left out to simplify the figure.

NOTE 2: The OSF consists of S-OSF, N-OSF and Network Element - Operations System Function (NE-OSF) and has a relationship to every functional elements in its domain.

Figure B.1: IN distributed functional plane model for CS2

B.1.1 End user access

End user can access IN functionality via various means, like analogue line interfaces, Integrated Services Digital Network (ISDN) Basic Rate Interface (BRI) or Primary Rate Interface (PRI), Public Land Mobile Network (PLMN) mobile access, private network access, Broadband Integrated Services Digital Network (B-ISDN) customer or trunk access, or traditional trunk and Signalling System No.7 (SS7) interfaces.

B.1.2 Service invocation and control

Call/service processing for CS2 builds upon the current call processing infrastructure of existing digital exchanges. It does so by using a generic model of existing call control functionality to process basic two-party calls, then adding service switching functionality to invoke and manage IN service features. Once invoked, IN service features are executed under the control of service control functionality, in conjunction with service data functionality. With this distributed approach to call/service processing, the existing call control functionality retains ultimate responsibility for the integrity of calls, as well as for the control of call processing resources.

There will be a set of constraints that apply to CS2, including:

a) CCF and SSF are tightly coupled, hence no relationship between those entities is standardized in CS2;

b) a call can be initiated by an end user or by a SCF on behalf of an end user;

c) a call may span multiple exchanges.

B.1.3 End user interaction with service control

End user interaction with the network to send and receive information is provided by service switching and call control resources, augmented by specialized resources. These specialized resources are controlled by service control functionality, and are connected to end users via call control and service switching functionality.

B.1.4 IN management

IN management functionality will be used to provide and manage service creation, the service control functionality, service data functionality, specialized resource functionality and the combined service switching/call control functionality in the network, outside the context of call/service processing. The IN management functions are modelled according to the TMN functional architecture. The end user may access the management facilities via a direct link to TMN systems, or as part of management features implemented in the SCF service logic. The entity OSF in figure B.1 should be seen to represent the full TMN capability, including Element Management, Network Management and Service Management functionality (E-OSF, N-OSF and S-OSF, respectively). IN management is described in more detail in the main part of this ETR.

B.1.5 Inter working between service processing functional entities

Service features, distributed over different service processing entities, may interwork/co-operate to provide a service to an end user. This can be the case when a service spans multiple networks or when a specific feature of a service is distributed in the network, for example for performance reasons. Although different service processing entities may be involved at the same time for one service, at any time only one service processing entity controls the call processing resources. The main part of this ETR deals with interworking in more detail.

B.2 Functional description of each component

B.2.1 CCAF

CCAF is the Call Control Agent (CCA) function that provides access for users. It is the interface between user and network Call Control Functions (CCF). It:

a) provides for user access, interacting with the user to establish, maintain, modify and release, as required, a call or instance of service;

b) accesses the service-providing capabilities of the Call Control Function (CCF), using service requests (i.e. set-up, transfer, hold etc.) for the establishment, manipulation and release of a call or instances of service;

c) receives indications relating to the call or service from the CCF and relays them to the user as required;

d) maintains call/service state information as perceived by this functional entity.

B.2.2 CCF

CCF is the call control function in the network that provides call/connection processing and control. It:

a) establishes, manipulates and releases call/connection as "requested" by CCAF;

b) provides the capability to associate and relate CCAF functional entities that are involved in a particular call and/or connection instance (that may be due to SSF requests);

c) manages the relationship between CCAF functional entities involved in a call (e.g. supervizes the overall perspective of the call and/or connection instance);

d) provides trigger mechanisms to access IN functionality (e.g. passes events to the SSF).

B.2.3 SSF

SSF is the service switching function, which, associated with the CCF, provides the set of functions required for interaction between the CCF and a SCF. It:

a) extend the logic of the CCF to include recognition of service control triggers and to interact with the SCF;

b) manages signalling between the CCF and the SCF;

c) modifies call/connection processing functions (in the CCF) as required to process requests for IN provided service usage under the control of the SCF;

d) for mobile subscribers, a handover procedure between SSFs may be required The SCF needs to be aware when the handover takes place, either by requesting the handover or by receiving an indication. This will require a new type of event. If this should be possible for all phases of a call, is for further study.

B.2.4 SCF

SCF is a function that commands call control functions in the processing of IN provided and/or custom service requests. The SCF may interact with other functional entities to access additional logic or to obtain information (service or user data) required to process a call/service logic instance. It:

a) interfaces and interacts with SSF/CCF, SRF, SCAF and SDF entities;

b) contains the logic and processing capability required to handle IN provided service attempts. These service attempts can be either call associated or non-call associated (e.g. location updating or registering of a mobile subscriber);

c) interacts with other SCFs, if necessary. Interaction with other SCFs is based on different requirements:

- different services, to resolve interaction between different services in different SCFs;
- one service, one service could span different SCFs because of network boundaries or because the service requires distributed control (e.g. relevant parts of the service are distributed and a part of the network resources is allocated to their control);
- to provide access to the SSF/CCF capabilities to a different SCF, which can or may not access the SSF/CCF directly.

B.2.5 SDF

SDF contains customer and network data for real time access by the SCF in the execution of an IN provided service. It:

a) interfaces and interacts with SCFs as required;

b) interfaces and interacts with other SDFs; this allows distribution of data management functionality and location transparency for data manipulation. Access to data in the SDF from the SCF requires no knowledge in the SCF with respect to the location of the data (distributed database functionality).

NOTE: The SDF contains data relating directly to the provision or operation of IN provided services. Thus it does not necessarily encompass data provided by third party such as credit information, but may provide access to these data.

Security on the SDF interface is provided by means of access rights, the SDF will verify the access rights of an interacting SCF or SDF with respect to the accessed data.

The SDF is service independent in the same way as the SCF. When a new service is too be introduced, the SCF and the SDF are not functionally modified. or the SCF, the Service logic will contain the service specific part. For the SDF, the service specific part will be a Service data template. The SDF may provide more than data access, it can process functional requests from the SCF to process certain data.

To provide secure data access, unsuccessful comparisons can be monitored and data access can be denied if too many unsuccessful attempts are detected. Also call record handling, billing, authentication and security should be considered.

The SDF provides for the functionality required for distributed data management. this involves data location management for accessing data in another SDF and for distribution of data to other SDFs, maintaining data integrity for data which is distributed/copied to other SDFs. The security functions, required to enable secure access to distributed data, are also provided by the SDF.

B.2.6 SRF

SRF provides the specialized resources required for the execution of IN provided services (e.g. digit receivers, announcements, conference bridges, protocol converters like fax or modem conversion, etc.). It:

a) interfaces and interacts with SCF and SSF (and with the CCF);

b) may contain the logic and processing capability to receive/send and convert information received from users;

c) may contain functionality similar to the CCF to manage bearer connections to the specialized resources.

B.2.7 SCUA

SCUA is the Service Control User Agent that provides access for users. It is the interface between user and network service control functions. It:

a) provides for user access, interacting with the user to establish, maintain, modify and release, as required, an instance of service;

b) accesses the service invocation capabilities of the SCAF, using service requests (e.g. location registration, attach, etc.) for the invocation of non-call associated services;

c) receives indications relating to non-call associated services from the SCAF and relays them to the user as required;

d) maintains service state information as perceived by this functional entity.

B.2.8 SCAF

SCAF is the function, which, associated with the Service Control User Agent Function (SCUAF), provides the set of functions required for access and interaction between the user and a Service Control Function (SCF) for non-call associated services. It:

a) extends the logic of the SCUAF to include recognition of service control triggers and to interact with the SCF;

b) manages/polices signalling between the SCUAF and the SCF;

c) receives indications relating to the service from the SCF and relays them to the SCUAF as required;

d) maintains call/service state information as perceived by this functional entity.

Annex C: Threat analysis of the core INAP information flows

This annex provides an analysis of the information flows between IN entities from a security point of view. The analysis is based on Core INAP (ETS 300 374-1 [1]) and CS1 Distributed Functional Plane (ETR 318 [2]). INAP is a protocol that supports interactions between the following functional entities defined in the IN model: SSF, SCF, SRF and SDF. OSF is not included. Note that Core INAP only covers CS1.

The meaning and importance of the various elements of the information flow are shown in table C.1. The masquerading column indicates what the originator or recipient can gain by masquerading, e.g. a network provider could ask for call information from a competitor's SSF. Integrity threat indicates that the mentioned party could benefit by altering the information in the operation (as opposed to reading the information as in content sensitivity). Identified roles are User, Subscriber, Service Provider (SP) and public or private NO. Content sensitivity is either high, medium or low, depending on the information conveyed through the operation. The criteria for choosing the level of sensitivity has been the following: if the information contains private or confidential data, High sensitivity has been chosen; if the information flow contains addresses, reference numbers or charging data, Medium sensitivity has been chosen; Low sensitivity has been chosen for all release information and when no parameters are conveyed in the operation.

Table C.1: Meaning and importance of the information flow components

Operation/Info flow	Direction	Sensitivity		
		Masquerade threat from	**Integrity threat from**	**Content sensitivity**
SCF ↔ SSF				
Activate Service Filtering	SCF→SSF	Originator	SP	Medium (Charging & Addresses)
Activity Test	SCF→SSF	Recipient		Low
Activity Test Response (Return result from Activity Test)	SSF→SCF	Originator		Low
Apply Charging	SCF→SSF	Originator	Subscriber User SP NO	Medium (Charging)
Apply Charging Report	SSF→SCF	Originator	Subscriber User SP NO	Medium (Charging)
Call Gap	SCF→SSF		SP PNO	Medium (Addresses & Control)
Call Information Report	SSF→SCF		SP NO	Medium (Addresses & statistics)
Call Information Request	SCF→SSF	Originator		Low
Collect Information	SCF→SSF			Low
Connect	SCF→SSF			Medium (Addresses)
Connect to Resource	SCF→SSF	Originator Recipient	SP NO	Medium (Addresses)
Continue	SCF→SSF	Originator		Low
Disconnect Forward Connection	SCF→SSF	Originator		Low
Establish Temporary Connection	SCF→SSF	Originator?		Medium (Addresses)
Event Notification Charging	SSF→SCF			Medium (Charging)
Event Report Basic Call State Model (BCSM)	SSF→SCF	Recipient		Medium (Addresses)

(continued)

Table C.1 (concluded): Meaning and importance of the information flow components

Operation/Info flow	Direction	Sensitivity		
		Masquerade threat from	**Integrity threat from**	**Content sensitivity**
SCF ↔ SSF				
Furnish Charging Information	SCF→SSF	Originator		Medium (Charging)
Initial DP	SSF→SCF	Originator Recipient		Medium (Addresses)
Initiate Call Attempt	SCF→SSF	Originator		Medium (Addresses)
Release Call	SCF→SSF	Originator		Low (Cause)
Request Notification Charging Event	SCF→SSF	Originator		Medium (ID's)
Request Report BCSM Event	SCF→SSF	Originator?		Medium (ID's)
Reset Timer	SCF→SSF	Originator	-	Low (Medium)
Send Charging Information	SCF→SSF	Originator	User Subscriber SP NO	Medium (Charging)
Service Filtering Response	SSF→SCF	Recipient?	-	Low
SCF ↔ SRF				
Assist Request Instructions	SSF/SRF→SCF	Originator?		Low (ID's)
Cancel	SCF→SRF	Originator		Low
Collected User Information (Return result from Prompt and collect user information)	SRF→SCF	Originator Recipient	User Subscriber SP NO	High (Data)
Play Announcement	SCF→SRF	Originator	SP NO	Low (Control)
Prompt and collect user information	SCF→SRF	Originator Recipient	User Customer SP NO	High (Data)
Specialized Resource Report	SRF→SCF		-	Low (Null)
SCF ↔ SDF				
Update	SCF→SDF	Originator Recipient?	User Subscriber SP NO	High
Return Result from Update	SDF→SCF	Recipient Originator?		Medium
Screen	SCF→SDF	Originator Recipient	User Subscriber SP NO	High (Data)
Return Result from Screen	SDF→SCF	Recipient Originator	User Subscriber SP NO	High (Result)
Retrieve	SCF→SDF	Originator Recipient?	-	Medium
Return Result from Retrieve	SDF→SCF	Recipient Originator?	User Subscriber SP NO	High

NOTE: The SCF-SDF relationship is not yet stable in Core INAP.

Annex D: Bibliography

EU document SYN 287 (1992): "Amended proposal for a council directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data".

History

Document history	
November 1996	First Edition

ISBN 2-7437-1093-4
Dépôt légal : Novembre 1996